CMPT 352 Midterm 2006 Exam NAME: ______________________

80 Mins CLOSED BOOK

Do all 9 questions for 62 marks. Student#: ______________________

Use POINT FORM wherever possible. Use this paper (there is lots of room on the back). Please ask for an exam booklet if you need one. Budget your time as you could easily spend too long on a short question! If you are not sure what is meant by a question, or you spot a problem in the exam, write me a note about it and then make an assumption, and answer the question based on the assumption you have made (and stated). Closed Book - no books, notes or electronic devices allowed.

1. (3 marks) When a workstation connected to a LAN reads all frames or packets going past it even though they are not addressed to it, the workstation is in

   Promiscuos mode.

2. (3 marks) True or False: "Having a low-profile, little-known Web site makes it far less likely that your Web site will be attacked by hackers." Briefly indicate the reason you chose your answer:

   false, as Security is important to all organizations. The site may be a favored target for amatuer Hackers if it's thought to have Poor security. ([illegible])

3. (3 marks) True or False: "nMap can usually tell what version of Windows is being ran on a targeted host." Briefly indicate the reason you chose your answer:

   True. Although it can give a vauge answer with an -T scan, an -sV scan will give service versions, and that would help deduce the exact OS. ([illegible])

4. (3 marks) True or False: "Determining the current operating system, web-server version, and the update history of a web site, while valuable to an attacker, is usually difficult to do." Briefly indicate the reason you chose your answer:

   false. This can be done by routine scans using nMap, or a website such a Netcraft

5. (3 marks) True or False: "Many of the same legal issues arise when monitoring employee activity on a Web site and monitoring customer or visitor activity on the same Web site." Briefly indicate the reason you chose your answer:

False, Although Privacy issues are called in to question in Both cases, an employee is often using work property and how that property is used is the right of the employer to know, whereas a customer may be at home, and their info is generally used for demographics.

6. (5 marks) What is "network sniffing"? Name three (3) typical counter measures to limit the danger or to discover the presence of an unauthorized sniffer?

Definition: Studying all packets on a network despite not being addressed to the computer.

Counter measures: Avoid using Wireless Networks.
Do physical monitoring of network Jacks.
Encrypt packets before transmission

7. (30 Marks – 3 marks each) Briefly define the following terms we have discussed in the field of infoSec (an example may help but is not required) AND explain the importance or use in information technology security:

What is "wild"?

a. The wild list:

Definition: A list of "wild" Viruses

Importance/Use: This website will keep an account of when a particular virus is found on a participating system so InfoSec personell can be kept up to date on threats

b. Scan:

Definition: Trying to get informaton from multiple targets. may be multiple probes,

Importance/Use: To find ~~[illegible]~~ all information of a system. This may be done during an audit to see if any confidental info may be revealed.

c. War driving:

Definition: Driving around trying to detect a wireless network.

Importance/Use: In the most harmless case, it could be used by someone checking their email, in a more malicios case it could be used to initiate a DDos attack to prevent an attacker from being traced to their home.

d. Polymorphic virus:

Definition: A virus that has multiple forms.

2

Importance/Use: This can be Used to make a more serious attack on unsuspecting systems.

e. Dumpster diving:

Definition: Looking through garbage to locate confidentian information, like Names or passwords.

Importance/Use: If a person located a list of passwords, it could ease the hacking process. It a list of emploxees was found, it could be used in conjundion with Social Engearing.

f. Convergence:

Definition: ______________________________

____

Importance/Use: ______________________________

____

____

g. Evil Twin attack on a wireless network

Definition: Using another route with stronger signal to get other computers to connect to it.

Importance/Use: If a computer connected to it instead of the correct router, it could give away about how to authenticate to the correct Network.

h. Risk Management

Definition: To identify and Protect against risks.

Importance/Use: This is done to find threats, the likelihood of threats and compare the cost of protection and the cost of recovering from a threat.

i. Common Descriptive Language (Taxonomy)

Definition: A common definiton that experts in a field will accept.

Importance/Use: This is important in order to clear up ambigues terms and ideas, for example stealing a file over copying a file.

j. Social Engineering

Definition: Using deception to get what you want.

Importance/Use: for example, calling up an IT Dept and saying you forgot a password, and Pretending to be an employee.

8. (6 marks) List three themes that have repeated throughout the history of infoSec

CIA - confidently, Accessability, Integrity.

Risk management - Identify risks.

Hardware is easy to secure, People and Procedure is difficult.

9. (6 marks) List and briefly explain the 6 atomic elements of INFOSEC according to the model described by Donn Parker (an example, while not required, may help your explanation).

Confidentuality ✓

Authentication ✓

Utility ✓

Accessability ✗

Integrity ✓

Posession ✓